REMARKS

Claims 1-67 are pending in the present application. Claims 13, 25, 38 and 59 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. Figures

In a phone call with the Examiner on 08/17/05, Applicants' representative confirmed with the Examiner that the comment on page 2, item #6 of the present Office Action (with respect to the figures) was inadvertently included in the Detailed Action section of such Office Action (as Figure 6 does not make mention of Figure 6a-e). Thus, Applicants are disregarding this comment in the present response.

II. 35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 1-12, 22-24, 26-37, 45 and 47-58 under 35 U.S.C. § 103 as being unpatentable over Conklin et al (5,991,881 A) in view of Cozza (5,473,769 A). This rejection is respectfully traversed.

With respect to Claim 1, it is urged that none of the cited references teach or suggest the claimed feature of "journaling the data to form journaled data, wherein journaling the data comprises *maintaining a previous state of the data for subsequent, optional restore of the data to the previous state*". As can be seen, the claimed journaling of data is with respect to data that can be restored to a previous state. None of the cited references teach or otherwise suggest such journaling of data, and thus it necessarily follows that none of the cited references teach or otherwise suggest the claimed steps of "determining whether a virus is present in the data processing system *after journaling of the data has begun*" (since there is no teaching of journaling of data), or "responsive to an identification of the virus, *restoring the data using the journaled data*" (since there is no teaching of the claimed journaled data). These claimed features advantageously provide an ability to repair damage caused by an unauthorized intrusion of a data processing system, and accomplishes this advantage by pro-actively journaling data such that it can be restored in the event of such unauthorized intrusion.

None of the cited references teach or suggest the claimed features described above, or their resulting advantages. The cited Conklin reference teaches a system that logs network traffic data upon detection of an unauthorized intrusion, but does not teach or otherwise suggest *journaling of data prior to detecting a virus,* or *restoring data* using the journaled data. The cited Cozza reference is concerned about the length of time it takes to perform a scan of viruses in a computer system, and is specifically directed to particular virus scanning techniques that reduce the scan time. This reference does not teach any type of data restore operation that uses journaled data.

In rejecting Claim 1, the Examiner acknowledges that the cited Conklin reference does not disclose restoring the data using journaled data, but states that Cozza discloses restoring the data using the journaled data at col. 2, lines 49-67. Applicants urge that there, Cozza states:

> "The method and apparatus of the present invention for scanning files for computer viruses relies on the fact that viruses invariably change the file or volume they infect. Consequently, information detailing the initial "state" of an uninfected file or volume can be "cached" or securely saved to disk or other non-volatile storage medium. The cached information is dependent not only on the type of machine the scanning program is running on, but also on viruses' method of infection on that type of machine. The stored information can be tailored to meet the variety of situations found in present and future computing environments.
>
> Once the initial "state" information has been stored to a disk or other non-volatile storage medium, the method and apparatus of the present invention can use this cached information in future virus scans to determine what files and/or volumes have changed in a way indicative of most virus infections. In many applications this information alone is enough to eliminate the need to scan a file/volume for most, if not all, viruses."

As can be seen, this passage describes a technique for *scanning files* for a virus. It does not describe in any way subsequent data restore actions that are performed as a result of detecting a virus. As a part of this Cozza volume scan operation, information detailing the initial "state" of an uninfected file or volume is cached or saved to disk such that is can be used when comparing a current state of a file or volume during a scan of the file/volume *in order to determine what files or volumes have changed.* Thus, this technique is specifically directed to a way of scanning a file/volume to reduce the time it takes for such scan, because in many instances, this information alone is enough to eliminate the need to scan a file/volume for most, if not all, viruses. This cited passage does not describe any action – such as restoring data using journaled data – that results from detection of a virus. Claim 1 expressly recites "responsive to an identification of the virus, restoring the data using the journaled data".

This missing claimed feature is also evidenced by Cozza's Figure 4, block 58, where a check is made as to whether there are any viruses. If yes, the file cache entry is zeroed out and the file scan ends. The process then loops to the next file on the volume to be scanned. Thus, *the only action described by Cozza that is responsive to an identification of a virus is to zero the file cache entry*. This is described at Cozza col. 5, lines 23-26 and col. 4, lines 20-21, where this operation zeroes out the cache such that the file will be completely scanning in the future. Such zeroing of the cache does not teach or otherwise suggest the claimed feature of "responsive to an identification of the virus, *restoring the data using the journaled data*". It is thus urged that a proper prima facie case of obviousness has not been established with respect to Claim 1, as there are claimed features not taught or suggested by the cited references[1]. Accordingly, the burden has not shifted to Applicants to rebut obviousness[2]. It is thus shown that Claim 1 has been improperly rejected under 35 USC 103[3].

---

[1] To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974).

[2] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id.

[3] If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

With respect to Claims 2-12, Applicants initially traverse for reasons given above with respect to Claim 1 (of which Claims 2-12 depend upon).

Further with respect to Claim 2, Applicants urge that none of the cited references teach or otherwise suggest the claimed feature of "responsive to an absence of an identification of the virus, discarding the journaled data". In rejecting Claim 2, the Examiner cites Conklin Figures 6 and 7 and associated text as teaching this claimed step. Applicants urge that while these figures show a discard box and describe an associated discard operation being performed if no virus is identified, the item that is discarded is the data packet that is received from the network and examined for a potential virus (col. 5, lines 22-25). A teaching of discarding a received data packet from a network, as described by Conklin, does not teach or otherwise suggest *discarding of the journaled data*, as expressly recited in Claim 2. Thus, Claim 2 is further shown to have been improperly rejected, as a proper prima facie showing of obviousness has not been established.

Further with respect to Claim 8, Applicants urge that none of the cited references teach or otherwise suggest the claimed feature of "responsive to an identification of the virus, blocking access to the data by a process accessing the data". In rejecting Claim 8, the Examiner cites Conklin's teaching at col. 5, lines 34-38 as disclosing this claimed feature. Applicants urge that this cited passage describes writing triggering packets to a log file for subsequent processing. Such writing of packets to a log file for subsequent processing does not teach or otherwise suggest *blocking* access to the data, as expressly recited in Claim 8. Thus, Claim 8 is further shown to have been improperly rejected, as a proper prima facie showing of obviousness has not been established.

Further with respect to Claim 9, Applicants urge that none of the cited references teach or otherwise suggest the claimed feature of "responsive to an identification of the virus, generating an indication halting a process accessing the data". In rejecting Claim 9, the Examiner cites Conklin's teaching at col. 5, lines 22-44 as teaching this claimed step. Applicants urge that there, Conklin states:

> "If, there is no indication of an actual or potential intrusion, then the examined packet data is discarded. When a packet or accumulation of

> packets match a predefined intrusion profile the Intrusion Detection function identifies the network traffic as a reportable activity will construct a data structure which contains a date/time stamp indicating the time of detection, the source and destination Internet Protocol (IP) addresses, an assigned message identifying the event detected. This data structure is passed to the Alert Notification function for processing. When a positive identification of a reportable activity occurs, the entire triggering packet(s) may be written to a log file created in the Evidence Logging function. This log file is then used to hold all ensuing packets associated with this reportable activity event by any one of its identifiable characteristics. For example, the log file written is named using the date/time and name of event detected. The source Internet Process (IP) address is sent to the Evidence Logging function as a controlling parameter so that a secondary logging function may be started which will only capture packets to and from the IP address identified as the source of the intrusion or attack."

As can be seen, when a packet matches an intrusion profile, (1) the network traffic is identified as a reportable activity, (2) a data structure is created which contains information pertaining to the packet, which is passed to the Alert Notification function for processing, (3) the triggering packets are written to a log file for subsequent processing, and (4) a secondary logging function is started which only captures certain subsequent packets. This passage makes no mention of any type of halting operation, and thus does not teach or otherwise suggest the claimed step of "responsive to an identification of the virus, generating an indication halting a process accessing the data". Thus, Claim 9 is further shown to have been improperly rejected, as a proper prima facie showing of obviousness has not been established.

Further with respect to Claim 10, Applicants urge that none of the cited references teach or otherwise suggest the claimed feature of "wherein the journaled data is accessed by a single process and maintained until a determination is made that the single process is eliminated as a virus candidate". In rejecting Claim 10, the Examiner cites Conklin's

teaching at figure 6 and associated text as disclosing this claimed feature. Applicants urge that this cited portion of Conklin does not describe any type of process eliminiation technique, and specifically does not describe any method of eliminating as a virus candidate *the process that is accessing journaled data*. For example, Conklin is examining data packets received across a network for viruses, and is not examining or making virus determinations with respect to internal processes themselves, and thus is not making any type of virus determination with respect to a process that is accessing journaled data, as expressly recited in Claim 10. Thus, Claim 10 is further shown to have been improperly rejected, as a proper prima facie showing of obviousness has not been established.

With respect to Claim 11, none of the cited references teach or suggest the claimed feature of "wherein the *journaled data* is stored in a protected memory accessible only by the method". In rejecting Claim 11, the Examiner cites Conklin's teaching at figure 9 and associated text as disclosing this claimed feature. Applicants urge that since Conklin does not teach or suggest "journaled data" (which is specifically defined in Claim 1, of which Claim 11 depends upon, and is shown above to not be taught by Conklin in the Claim 1 discussion), it necessarily follows that Conklin does not teach storing such (missing) journaled data in a particular place, as per Claim 11. Thus, Claim 11 is further shown to have been improperly rejected, as a proper prima facie showing of obviousness has not been established.

With respect to Claim 12, none of the cited references teach or suggest the claimed feature of "wherein the *journaled data* is stored in a data structure located in a protected memory inaccessible by a process" for similar reasons to those given above with respect to Claim 11. Thus, Claim 12 is further shown to have been improperly rejected, as a proper prima facie showing of obviousness has not been established.

With respect to Claims 22-24 and 26-37, Applicants initially traverse for similar reasons to those given above with respect to Claim 1.

Further with respect to Claim 27, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 2.

Further with respect to Claim 33, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 8.

Further with respect to Claim 34, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 9.

Further with respect to Claim 35, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 10.

Further with respect to Claim 36, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 11.

Further with respect to Claim 37, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 12.

With respect to Claim 45, the Examiner provided no reasoning for the rejection of such claim under 35 USC 103. Further clarification is requested as to the specific basis for rejecting such claim under 35 USC 103.

With respect to Claims 47-58, Applicants initially traverse for similar reasons to those given above with respect to Claim 1.

Further with respect to Claim 48, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 2.

Further with respect to Claim 54, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 8.

Further with respect to Claim 55, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 9.

Further with respect to Claim 56, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 10.

Further with respect to Claim 57, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 11.

Further with respect to Claim 58, Applicants further traverse for similar reasons to those further reasons given above with respect to Claim 12.

Therefore, the rejection of Claims 1-12, 22-24, 26-37, 45 and 47-58 under 35 U.S.C. § 103 has been overcome.

III. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 13-21, 25, 38-44, 46 and 59-67 under 35 U.S.C. § 102(b) as being anticipated by Conklin et al (5,991,881 A). This rejection is respectfully traversed.

With respect to Claim 13 (and dependent Claims 14-21), Applicants urge that the cited reference does not teach the claimed step of "saving a state of a data object *in response to a request to access the data object by a process*", which is in addition to the claimed step of "performing pattern matching of a set of actions taken within the data processing system". Applicants urge that the cited reference does not teach, nor has the Examiner alleged any teaching of, both pattern matching of a set of actions *and saving a state of a data object in response to a request to access the data object by a process*. Thus, as every element of the claimed invention is not identically shown in a single reference, it is shown that Claim 13 (and dependent Claims 14-21) is not anticipated by the cited reference. In any event, Claim 13 has been amended to further distinguish over the teachings of the cited reference. It is urged that the cited reference does not teach any type of rollback operation, for similar reasons to those given above with respect to Claim 1.

Further with respect to Claim 15, Applicants urge that the cited reference does not teach the claimed feature of "*if an intrusion is absent*, determining whether a time threshold has been reached; and if an absence of a reaching of the time threshold is present, repeating the matching step using another set of actions". In rejecting Claim 15, the Examiner cites the teaching of Conklin at Figure 6-8 and associated text and col. 6, lines 60-63 as teaching this claimed feature. Applicants urge that none of the cited passages describe any type of time determination being made *if an intrusion is absent*, and thus none of these cited passages teach or otherwise suggest determining whether a time threshold has been reached, any actions resulting from such (missing) determination. Instead, Conklin states that continuous logging occurs until no packets are written for a predetermined period of time – and this logging is *in response to an intrusion being detected* (col. 6, lines 45-63), which is exactly opposite to the responsive event ("if an intrusion is absent") recited in Claim 15. Thus, Claim 15 is further shown to not be anticipated by the cited reference.

Applicants traverse the rejection of Claims 25, 38-44 and 46 for similar reasons to those given above with respect to Claim 13.

Further with respect to Claim 40, Applicants further traverse the rejection of such claim for similar reasons to the further reasons given above with respect to Claim 15.

Applicants traverse the rejection of Claims 59-67 for similar reasons to those given above with respect to Claim 13.

Further with respect to Claim 61, Applicants further traverse the rejection of such claim for similar reasons to the further reasons given above with respect to Claim 15.

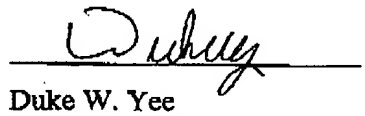
Therefore, the rejection of Claims 13-21, 25, 38-44, 46 and 59-67 under 35 U.S.C. § 102 has been overcome.

IV. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 8/18/05

Respectfully submitted,



Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants